US009524393B2

(12) **United States Patent**
Aggarwal et al.

(10) **Patent No.: US 9,524,393 B2**
(45) **Date of Patent: Dec. 20, 2016**

(54) **SYSTEM AND METHODS FOR ANALYZING AND MODIFYING PASSWORDS**

(71) Applicant: **The Florida State University Research Foundation, Inc.**, Tallahassee, FL (US)

(72) Inventors: **Sudhir Aggarwal**, Tallahassee, FL (US); **Shiva Houshmand Yazdi**, Tallahassee, FL (US); **Charles Matt Weir**, Tallahassee, FL (US)

(73) Assignee: **The Florida State University Research Foundation, Inc.**, Tallahassee, FL (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 101 days.

(21) Appl. No.: **14/266,277**

(22) Filed: **Apr. 30, 2014**

(65) **Prior Publication Data**

US 2014/0373088 A1 Dec. 18, 2014

Related U.S. Application Data

(63) Continuation of application No. PCT/US2012/062730, filed on Oct. 31, 2012.

(60) Provisional application No. 61/553,554, filed on Oct. 31, 2011.

(51) **Int. Cl.**
G06F 21/60 (2013.01)
G06F 21/46 (2013.01)

(52) **U.S. Cl.**
CPC ***G06F 21/604*** (2013.01); ***G06F 21/46*** (2013.01)

(58) **Field of Classification Search**
CPC G06F 21/604; G06F 21/46
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,539,247 B2 * 9/2013 McGrew G06F 21/46 713/182
8,769,607 B1 * 7/2014 Jerdonek G06F 21/31 726/1
9,178,876 B1 * 11/2015 Johansson H04L 63/0846
2008/0063192 A1 3/2008 Goubin et al.
(Continued)

OTHER PUBLICATIONS

Aggarwal, et al., "Building Better Passwords using Probabilistic Techniques", ACSAC '12, Dec. 3-7, 2012, Orlando, Florida USA.*
(Continued)

Primary Examiner — Joseph P Hirl
Assistant Examiner — J. Brant Murphy
(74) *Attorney, Agent, or Firm* — Nilay J. Choksi; Smith & Hopen, P.A.

(57) **ABSTRACT**

A system for analyzing and modifying passwords in a manner that provides a user with a strong and usable/memorable password. The user would propose a password that has relevance and can be remembered. The invention would evaluate the password to ascertain its strength. The evaluation is based on a probabilistic password cracking system that is trained on sets of revealed passwords and that can generate password guesses in highest probability order. If the user's proposed password is strong enough, the proposed password is accepted. If the user's proposed password is not strong enough, the system will reject it. If the proposed password is rejected, the system modifies the password and suggests one or more stronger passwords. The modified passwords would have limited modifications to the proposed password. Thus, the user has a tested strong and memorable password.

14 Claims, 7 Drawing Sheets